UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

Robert Ayers, on his own behalf and on behalf of those similarly situated, Plaintiff, v. Fred Hutchinson Cancer Center, Defendant.	Case No.: **COMPLAINT – CLASS ACTION** (Jury Trial Demanded)

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

Plaintiff Robert Ayers ("Plaintiff"), by and through his attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information as to all other matters, files this complaint against Defendant and alleges the following.

INTRODUCTION AND NATURE OF ACTION

1. Plaintiff brings this class action complaint on behalf of himself and a class of persons ("Class Members") harmed by Defendant Fred Hutchinson Cancer Center's ("Fred Hutchinson" or "Defendant") failure to safeguard, monitor, maintain and protect highly sensitive patient personal and health information, or Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information").

2. As a cancer center, Fred Hutchinson collects and maintains the Sensitive Information of an extremely vulnerable population of patients. On or about November 19, 2023, a malicious actor infiltrated Fred Hutchinson's data environment and successfully stole a host of patient information (the "Data Breach") from Defendant.

3. Weeks later, on December 1, 2023, Fred Hutchinson finally announced to the public that it had detected the unauthorized activity on its clinical network.[1] Although it has created a web page purportedly to provide updates regarding the Data Breach, Defendant has provided virtually no information to those whose information it put at risk with its insufficient data practices.

4. For example, in its "How did this happen?" section, Fred Hutchinson provides the evasive response that "all organizations face cybersecurity risks and these kind of attacks have targeted multiple healthcare institutions in the past."[2]

5. Far from absolving Fred Hutchinson of responsibility, the fact that healthcare institutions—including Fred Hutchinson—have been regularly targeted by hackers establishes the need for robust data security practices.

[1] https://www.fredhutch.org/en/news/releases/2023/12/notice-of-information-security-incident-involving-fred-hutchinso.html.
[2] https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

6. Further, in its "Is my information secure?" section, Fred Hutchinson merely claims that is "investigation is ongoing and we are continuing to assess the data involved, and that it "will contact any individuals whose information was involved."[3]

7. Defendant has not yet contacted the victims of its Data Breach. Unfortunately, however, many of the victims of the Data Breach, including Plaintiff, have already been contacted with confirmation that their data was exposed—by the hackers directly. In their extortionate emails to the victims, the hackers state, in part, the following:

> Fred Hutchinson Cancer Center was hacked on November 2023. The names, SSN, addresses, phone numbers, medical history, lab results, and insurance history of more than 800000 patients have been compromised. If you are reading this, your data has been stolen and will soon be sold to various data brokers and black markets to be used in fraud and other criminal activities.[4]

8. Included in the email directly from the hackers is evidence that the victims' information was in fact exfiltrated during the Data Breach, including the recipient's name, patient record number, insurer, and medical information.[5]

9. As a result of the lax security on Fred Hutchinson's network, Plaintiff and at least 800,000 other patients have had the most sensitive details of their lives and identities accessed and stolen by malicious cybercriminals.

10. Because the Data Breach compromised Plaintiffs' Sensitive Information, Plaintiff and the Class (defined below) have been placed in an immediate and continuing risk of identity theft related harm.

11. As a result of Fred Hutchinson's conduct, Plaintiffs and the Class have been and will be required to continue to undertake expensive and time-consuming efforts to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts

---

[3] *Id.*
[4] *See* https://news.yahoo.com/seattle-cancer-patients-face-blackmail-032107067.html.
[5] *See Id.*

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

for unauthorized activity, changing passwords on medical portals, and requesting and maintaining accurate medical records outside of those kept by medical providers. Minors may not be able to monitor the impact of the Data Breach on their lives for years, at which point the damage will be done and the minors will have to prove their identities.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, diversity is satisfied because at least one Class Member is a citizen of a different state than Defendant.[6] Further, Plaintiff alleges that in the aggregate the claims of all purposed class members exceed $5,000,000, exclusive of interest and costs.

13. This Court has jurisdiction over Defendant Fred Hutchinson Cancer Center because Defendant is located in Seattle, Washington. Defendant has sufficient minimum contacts with Washington because it conduct substantial business in the state.

14. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred within the Western District of Washington and because Defendant conducts a substantial part of its business within the Western District of Washington.

PARTIES

Plaintiff

15. Plaintiff Robert Ayers is a natural person and a citizen of the State of Washington. His permanent residence is in the State of Washington.

16. Plaintiff received medical treatment from Defendant. In connection with these medical services, Plaintiff provided Defendant with various forms of PHI and PII, including,

[6] *See* https://www.fredhutch.org/content/dam/www/clinical-pdf/housing/Housing-Guide.pdf, at 14 ("Fred Hutch welcomes many out-of-state patients.").

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

without limitation, name, address, social security number, date of birth, medical history, and medical insurance information. Through the services Plaintiff received, Fred Hutchinson created, maintained and stored additional PHI for Maynor, including, but without limitation, medical treatments or diagnoses, prescriptions, or insurance claim data.

17. Plaintiff is one of the numerous Fred Hutchinson patients whose PHI and PII was disclosed during the Data Breach. Following the Data Breach, Plaintiff received an email from the hackers providing a sample of the stolen data, warning Plaintiff that they had exfiltrated additional information, informing Plaintiff that he was one of more than 800,000 victims of the Data Breach, and threatening that his data would soon be sold to data brokers and black markets to be used in fraud and other criminal activities unless he paid an extortion fee.

Defendant

18. Defendant Fred Hutchinson Cancer Center is a Washington public benefit corporation, is a 501(c)(3) organization located at 1100 Fairview Ave N, King County, Seattle, WA 98109. Defendant's organization has eleven clinical locations in the State of Washington and three research locations in the United States, Uganda, and South Africa.

FACTUAL BACKGROUND

19. Founded in 1975, Fred Hutchinson Cancer Center conducts cancer and infection disease research and provides cancer treatment to patients. Billing itself as a leader in its areas, Defendant is a sizeable institution and employs more than 5,700 individuals.[7]

20. To obtain healthcare services, Fred Hutchinson requires patients to provide their PHI and PII. Defendant then compiles stores and maintains the highly sensitive PII and PHI. Defendant serves tens of thousands of individuals every year, indicating it has a massive repository of Sensitive Information, the kind of repository data thieves target.[8]

[7] https://www.fredhutch.org/en/about.html.
[8] https://www.fredhutch.org/en/about/about-the-hutch/annual-report.html.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

21. For example, in 2022 alone, Fred Hutchinson served over 53,000 patients and clients and had nearly 120,000 outpatient visits.[9]

22. Defendant also collects and stores data from patients who have never even been seen at a Fred Hutchinson location. Because Fred Hutchinson acts as the University of Washington's cancer center, it stores highly sensitive data from some University of Washington patients who have never been seen at Fred Hutchinson. These patients' data were involved in the Data Breach.[10]

23. Defendant advertises that it is "committed to respecting and upholding the privacy of every patient," and admits that it is covered by the Health Insurance Portability and Accountability Act, or HIPAA.[11] Defendant further maintains a "Notice of Privacy Practices" describing how patients' medical information will be used and disclosed.[12] Through its Notice, Fred Hutchinson admits to its patients that it is "required by law to maintain the privacy and security of your protected health information" and that it "will not use or share your information other than as described" in the Notice.[13] Defendant further promises patients that it "will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[14]

24. Plaintiff and the Class had a reasonable expectation that Fred Hutchinson would reasonably protect the Sensitive Information provided to it or created by it through the course of treatment. Fred Hutchinson had a legal obligation to reasonably safeguard the information against security breaches or other types of theft and misuse.

25. As described throughout this Complaint, Fred Hutchinson did not reasonably protect, secure, or store Plaintiffs' and the Class's Sensitive Information prior to, during, or after the Data Breach.

---

[9] *Id.*
[10] https://news.yahoo.com/seattle-cancer-patients-face-blackmail-032107067.html?guccounter=1.
[11] https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact.html.
[12] https://www.fredhutch.org/content/dam/www/utility/Joint-Notice-of-Privacy-Practices-Dec-19-2022.pdf.
[13] *Id.*
[14] *Id.*

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

I. The Data Breach

26. According to Fred Hutchinson, on November 19, 2023, Defendant became aware of unauthorized activity on its clinical network.[15] This network contained sensitive personal, medical, and insurance information of its current and former patients. Upon information, during this time, malicious actors gained unfettered access to Defendant's network and copied and exported substantial amounts of PII and PHI.

27. Defendant did not disclose the existence of the Data Breach to its patients or the general public until weeks later on December 1, 2023, long after it initially learned of the Data Breach. Defendant posted about the Data Breach on the "News Releases" section of its website[16] and created a "Data Security Incident" page on its website.[17] Defendant sent an email with similar information to all of its current and former patients, never confirming whose information was taken, or what information was accessed.

28. Defendant's email and website updates provide self-serving proclamations that Defendant is investigating the incident and shifting blame elsewhere, but contain scant information or guidance of use to the victims of the Data Breach. Defendant has provided no updates as to what, or whose, information was accessed during the Data Breach. Rather, the website updates recommended Plaintiff and the Class take several time-consuming steps to mitigate the risk of future fraud and identity theft, such as creating fraud alerts and credit freezes.

29. Defendant has not offered any credit monitoring or identity protection services. Instead, Defendant directs victims suspecting fraud or identity theft to contact the police, FTC, or FBI.[18]

30. Given that Defendant was storing the PII and PHI of Plaintiffs and the Class, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission or other agencies and required by

[15] https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html.
[16] https://www.fredhutch.org/en/news/releases/2023/12/notice-of-information-security-incident-involving-fred-hutchinso.html.
[17] https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html.
[18] https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

the Health Insurance Portability and Accountability Act. That obligation stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a host of highly sensitive patient records and data and, additionally, because of other highly publicized data breaches at healthcare institutions.

31. Fred Hutchinson had further reason to be protective of its patients' PHI and PII given a previous data security incident in which a Fred Hutchinson employee's email account was breached for two days in March 2022.[19]

32. The Data Breach itself and information Fred Hutchinson has disclosed to date indicates Defendant failed to implement reasonable measures to prevent cyber-attacks and the exposure of Sensitive Information including patient PHI and PII.

33. Despite the highly sensitive nature of the information Defendant created and stored, and the prevalence of health care data breaches, Defendant inexplicably failed to take appropriate steps to safeguard the PII and PHI of Plaintiffs and the Class from being compromised.

II. Data Breaches Lead to Identity Theft and Cognizable Injuries

34. The personal, health, financial, and insurance information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

35. Defendant's failure to reasonably safeguard Plaintiffs' and the Class's sensitive PHI and PII has created a serious risk to Plaintiffs and the Class, including both a short-term and long-term risk of identity theft.

36. Identity theft occurs when someone uses another's personal, financial, or similar information such as that person's name, account number, Social Security number, driver's license number, insurance information, date of birth, and/or other information, without permission, to commit fraud or other crimes.

[19] https://www.fredhutch.org/en/news/releases/2022/06/notice-of-a-data-security-incident-involving-seattle-cancer-care.html.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

37. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.[20]

38. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity. Hackers in this case have explicitly threatened victims that their information will indeed be sold to the dark web.

39. Moreover, according to Robert P. Chappell, Jr., a law enforcement professional, fraudsters can steal and use a minor's information until the minor turns eighteen years old before the minor even realizes he or she has been the victim of an identity theft crime.[21]

40. The risk to potential minor Class members is substantial given their age and lack of established credit. The information can be used to create a "clean slate identity," and use that identity for obtaining government benefits, fraudulent tax refunds, and other scams. There is evidence that children are 51% more likely to be victims of identity theft than adults.[22]

41. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and, tangible money, along with unreported emotional harms.

42. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone.

---

[20] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

[21] Brett Singer, *What is Child Identity Theft?*, Parents (last visited Jan. 17, 2022), https://www.parents.com/kids/safety/tips/what-is-child-dentity-theft/.

[22] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018) (last visited Jan. 18, 2022), https://axioncyber.com/data-breach/how-data-breaches-affect-children/.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

The same report identified "rapid reporting" as a tool to help law enforcement stop fraudulent transactions and mitigate losses.

43. Fred Hutchinson did not rapidly, or even reasonably, report to Plaintiffs and the Class that their Sensitive Information had been stolen.

44. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[23]

45. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;
(2) retaining payment card information only as long as necessary;
(3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;
(4) limiting administrative access to business systems;
(5) using industry unapproved activity;
(6) monitoring activity on networks to uncover unapproved activity;
(7) verifying that privacy and security features function property;
(8) testing for common vulnerabilities; and
(9) updating and patching third-party software.[24]

46. The United States Government and the United States Cybersecurity & Infrastructure Security Agency, recommends several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged

[23] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.
[24] *Start With Security, A Guide for Business,* FTC (last visited Jan. 18, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

47. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, reputation, and can take time, money and patience to resolve the effect.[25] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Fred Hutchinson failed to do here-- as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

III. The Healthcare Industry is Particularly Susceptible to Cyber Attacks.

48. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[26] According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.[27] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[28]

49. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate. [29]

---

[25] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[26] *See* Elinor Mills, *Study: Medical identity theft is costly for victims,* CNET (March 3, 2010), (last visited Jan. 11, 2021), https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

[27] *Id.*

[28] *Id.*

[29] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

50. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.[30] For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.[31]

51. As a healthcare provider having already experienced a recent cybersecurity incident and serving a highly vulnerable population of tens of thousands of patients each year, Defendant knew or should have known the importance of protecting the Sensitive Information entrusted to it. Defendant also knew or should have known of the foreseeable, and catastrophic consequences if its systems were breached. These consequences include substantial costs to Plaintiffs and the Class because of the Data Breach. Despite this, Defendant failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

IV. Plaintiff's and the Class's PHI and PII are Valuable.

52. Unlike financial information, like credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[32]

53. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an

[30] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[31] *Five worthy reads: The never-ending love story between cyberattacks and healthcare,* ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

[32] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

ongoing basis rather than exploiting just one account until it is canceled.[33] For that reason, Cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as $300 per number.[34] Those numbers are often then used for fraudulent tax returns.[35]

54. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[36] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

55. Fred Hutchinson's Data Breach exposed a variety of Sensitive Information, including, on information, Social Security numbers and PHI.

56. The Social Security Administration ("SSA") warns that a stolen Social Security number, can lead to identity theft and fraud: "Identify thieves can use your number and your credit to apply for more credit in your name."[37] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

57. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

---

[33] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[34] *Id.*

[35] *Id.*

[36] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

[37] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

58. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation ("FBI") has found instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.[38]

59. Other reports found that PHI is ten times more valuable on the black market than credit card information.[39] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for $1-2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute.[40]

60. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

61. Because the Sensitive Information exposed in the Fred Hutchinson Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their Sensitive Information.

V. Defendant's Conduct Violates HIPAA.

62. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of

[38] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

[39] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[40] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

information while protecting the privacy of people who seek care and healing.[41]

63. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[42] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[43]

64. HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8) Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[44]

65. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Fred Hutchinson failed to protect. The Data Breach resulted from Defendant's failure to comply with several of these standards:

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits;

b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

[41] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
[42] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html.
[43] *Id.*
[44] *Id.*

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

d. Violation of 45 C.F.R. § 164.308(a)(6)(ii): Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity

e. Violation of 45 C.F.R. §164.306(a)(2): Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information;

f. Violation of 45 C.F.R. §164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

g. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by its workforce;

h. Violation of 45 C.F.R. §164.502, et seq: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

i. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

66. Despite Defendant's failure to reasonably protect Plaintiffs' and the Class's Sensitive Information, it has not offered any compensation or remedy.

Plaintiff's Experience

67. Plaintiff Robert Ayers is a Washington citizen who is a former patient at Fred Hutchinson at the "Fred Hutch at UW Medical Center – Northwest" location. In order to obtain medical services from Defendant, Plaintiff was required to provide his PII and PHI to Defendant, including sensitive information including his name, address, date of birth, Social Security number, medical information, and insurance information. Additional highly personal health

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

information regarding Plaintiff Ayers was compiled throughout the course of his treatment with Defendant.

68. Plaintiff Ayers reasonably expected that his highly personal information would remain safeguarded and would not be accessible by unauthorized parties.

69. However, on or about December 6, 2023, Plaintiff learned of the Data Breach and the threat that his PII and PHI would be misused by unlawful actors. Defendant has not provided Plaintiff Ayers with any remedial measures.

70. Subsequent to and as a direct and proximate result of the Data Breach, Plaintiff received a frightening, extortionate, and anxiety-inducing email from hackers informing him that his information was taken during the Data Breach. Receiving this email, including its demand of payment and threat that his sensitive information would otherwise be sold and misused on the dark web, has caused Plaintiff Ayers a great deal of stress, worry, frustration, and anxiety.

71. Also subsequent to and as a direct and proximate result of the Data Breach, Plaintiff Ayers was alerted of a fraudulent charge of $1,300 to his bank account from Chicago, where Plaintiff Ayers does not live. Plaintiff Ayers was forced obtain a new bank card as a remedial measure.

72. Plaintiff Ayers is very careful about sharing his Sensitive Information. Plaintiff Ayers has never knowingly transmitted unencrypted Sensitive Information over the internet or any other unsecured channel. Plaintiff Ayers conscientiously takes reasonable precautions in order to preserve the security of his Sensitive Information.

73. Plaintiff Ayers suffered actual injury from having his sensitive information exposed and/or stolen as a result of the Data Breach, including: (a) required mitigation efforts, including needing to monitor banking and other accounts to ensure his information is not being used for identity theft and fraud; (b) damages to and diminution of the value of the Sensitive Information, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; (c) loss of privacy; (d) continuous imminent and impending injury arising from the

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

increased risk of financial, medical, and identity fraud and theft; and (e) time and expense of mitigation efforts required as a result of the Data Breach.

74. In addition, knowing that hackers accessed and exfiltrated his Sensitive Information and that this likely has been and will be used in the future for identity theft, fraud, and related purposes has caused Plaintiff Ayers to experience significant frustration, anxiety, worry, stress, and fear. These fears are heightened by the direct threats that he received from hackers at ransom due to Defendant's carelessness with his Sensitive Information.

75. Despite Defendant's failure to reasonable protect Plaintiff's and the Class's Sensitive Information, Defendant has not offered any compensation or adequate remedy, especially considering the significant and long-term risk Plaintiff and the Class Members face.

CLASS DEFINITION AND ALLEGATIONS

76. Plaintiff brings this class action pursuant to Federal Rule of Civil Procedure 23 and on behalf of themselves and all others similar situated, as representative of the following Class:

All persons whose Sensitive Information was exposed by the Data Breach.

77. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

78. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

79. Plaintiff's claims should be certified for class-wide treatment because Plaintiff can prove the elements of each claim on a class-wide basis and all members of the proposed Class are readily accessible through Defendants' records.

80. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

includes approximately, or more than, 800,000 people. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

81. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiff and Class members, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, without limitation:

a. Whether Defendant engaged in wrongful conduct alleged herein;

b. Whether the alleged conduct constitutes violations of the laws asserted;

c. Whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their Sensitive Information;

d. Whether Defendant breached its duty to protect the PII and PHI of Plaintiff and other Class members;

e. Whether Defendant knew or should have known about the inadequacies of its data protection, storage, and security;

f. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release, or disclosure;

g. Whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's offices and computer systems to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release or disclosure;

h. Whether Defendant's conduct was the proximate cause of Plaintiff's and the Class's injuries;

i. whether Plaintiff and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

j. Whether Plaintiff and the Class are entitled to recover damages; and

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

k. Whether Plaintiff and the Class are entitled to other appropriate remedies including injunctive relief.

82. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of himself and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

83. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's PHI and PII, like that of every other Class member, was misused and improperly disclosed by Defendant. Defendant's misconduct impacted all Class members in a similar manner.

84. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interest of the members of the Class, have retained counsel experienced in complex consumer class action litigation, and intend to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

85. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

86. Plaintiffs realleges and incorporates by reference every allegation contained in the paragraphs above, as though fully stated herein.

87. Defendant collected, created, and maintained Plaintiff's and the Class's Sensitive Information for the purpose of providing medical treatment to Plaintiff and the Class.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

88. Plaintiff and the Class are well-defined, foreseeable, and probable group of patients whom Defendant was aware, or should have been aware could be injured by inadequate data security measures. The nature of Defendant's business requires patients to disclose Sensitive Information to receive adequate care, including, without limitation, medical histories, dates of birth, addresses, phone numbers, and medical insurance information. Thus, for Defendant to provide its services, it is required to use, handle, gather, and store the Sensitive Information of Plaintiff and the Class, or alternatively, hire a third party to store and protect that data.

89. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that, given its repository of a host of Sensitive Information For hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

90. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information in its possession from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

91. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the Class's PHI and PII was adequately protected and secured.

92. Defendant also had a duty to timely disclose to Plaintiff and the Class that their Sensitive Information had been or was reasonably believed to have been compromised. Timely disclosure is necessary so that, among other things, Plaintiff and the Class could take appropriate measures to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

93. Additionally, HIPAA creates industry standards for maintaining the privacy of health-related data. Defendant knew or should have known it had a legal obligation to secure and protect Plaintiff's and the Class's Sensitive Information and that failing to do so is a serious violation of HIPAA.

94. Defendant also should have known that, given the Sensitive Information it held, Plaintiffs and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that their systems and technologies for processing and securing Plaintiff's and the Class's PHI and PII had security vulnerabilities susceptible to cyber-attacks.

95. Hackers successfully breached Defendant's network and data environments and stole a host of personal and healthcare information regarding, on information, hundreds of thousands of Defendant's patients.

96. Defendant, through its actions and/or omissions, systematically failed to provide reasonable security for the data in its possession.

97. Defendant breached its duty to Plaintiff and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiff's and the Class's PHI and PII, and failing to adequately disclose the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiff's and the Class's PHI and PII.

98. But for Defendant's wrongful and negligent breach of its duties, their Sensitive Information would not have been accessed and exfiltrated by unauthorized persons.

99. As a result of Defendant's negligence, Plaintiff and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE* (15 U.S.C. § 45)
(On Behalf of Plaintiff and the Class)

100. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above, as though fully stated herein.

101. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

102. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PHI and PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

103. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

104. Plaintiff and the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

105. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the proposed Class.

106. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have been injured as described herein and are entitled to damages in an amount to be proven at trial.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE* (HIPAA, 45 C.F.R. § 160.102)
(On Behalf of Plaintiffs and the Class)

107. Plaintiff realleges and incorporate by reference every allegation contained in the paragraphs above, as though fully stated herein.

108. Defendant required Plaintiff and the Class to provide nonpublic Sensitive Information to obtain medical services. Through the course of providing those services, Defendant created and stored even more PHI.

109. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

110. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information."

111. Per 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation specifications" apply to covered entities, such as Defendant. HIPAA standards are mandatory.

112. HIPAA requires Defendant to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably anticipated threats or hazards to the security or integrity" of the Sensitive Information. 45 C.F.R. § 164.306.

113. Defendant violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

114. Additionally, HIPAA requires timely notice of data breaches to each impacted consumer and defines timely as "in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. § 164.404. The notice must include certain minimum information, including, but not limited to, a description of the types of PHI that was accessed and a description of what the entity is doing to investigate the breach and mitigate harm. *Id.*

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

115. Defendant breached its HIPAA's notification duty by failing to give timely and complete notice. Indeed, the hackers themselves have already sent threatening messages to victims of the Data Breach, yet Defendant has not yet provided adequate notice to those same victims confirming whether or to what extent their Sensitive Information was affected.

116. Defendant violated HIPAA by failing to use reasonable measures to protect the PII and PHI of Plaintiffs and Class. Defendant's conduct was especially unreasonable given the nature of the Sensitive Information and the number of patients it serves, some of which are minors or patients who live below the federal poverty level or are dealing with illnesses, who may not have the means or health to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

117. Defendant's violation of HIPAA constitutes negligence *per se*. Plaintiff and the Class are within the group of individuals HIPAA was designed to protect and the harm to these individuals is a result of the Data Breach.

118. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON STATE DATA BREACH NOTIFICATION LAW (RCW 19.255)
(On Behalf of Plaintiffs and the Class)

119. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above, as though fully stated herein.

120. RCW 19.255.010, also known as the Washington State Data Breach Notification Law, mandates notice requirements for persons or businesses in Washington that suffer breaches of their computer systems.

121. Defendant conducts business within the State of Washington, and owns and collects data from its patients. This data includes personal information, including PHI and PII.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

Defendant is therefore required to comply with this section of the Washington State Data Breach Notification Law, RCW Chapter 19.255.

122. Pursuant to RCW 19.255.005, breach of the security system means "unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." The Data Breach is a breach of Defendant's security system, through which unauthorized persons acquired access to patients' personal information, including names, social security numbers, account numbers or credit or debit card numbers, date of birth, health insurance information, and medical histories, including diagnosis or treatment of the consumer, all of which is included within the definition for "personal information" provided within RCW 19.255.005(2).

123. RCW 19.255.010 requires any person or business that conducts business in Washington and that owns or licenses data that includes personal information to disclose any breach of the security of its data system to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. RCW 19.255.010(1).

124. The statute further requires any person or business that maintains or possesses data that may include personal information that the person or business does not own or license to notify the owner or licensee of the information of any breach of the security of its data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. RCW 19.255.010(2).

125. Businesses must also provide the required notice to affected consumers "in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered." RCW 19.255.010(8).

126. Business must include in their notice, among other things, "A list of the types of personal information that were or are reasonably believed to have been the subject of a breach." RCW 19.255.010(6).

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

127. According to Defendant's website, Defendant learned of the Data Breach on November 19, 2023. The Data Breach resulted in unauthorized access to the personal information, including, on information, PHI and PII of hundreds of thousands of Washington consumers.

128. In violation of this statute, Defendant has still not contacted affected consumers about the Data Breach to confirm to them whether, and what, of their personal information was affected. Defendant's delay certainly does not constitute notice "in the most expedient time possible," and does not meet the notice content requirements of RCW 19.255.010(6).

129. Pursuant to RCW 19.255.040(3)(a), any consumer injured by a violation of the Washington State Data Breach Notification Law may institute a civil action to recover damages. Businesses which violate this law may also be enjoined.

130. Defendant's violation of the provisions of this statute caused Plaintiffs and the Class injury. Defendant's delay has failed to provide guidance as to whether individual patients' PHI and PII was taken, or what specific information was taken, and therefore whether mitigatory steps are required. Defendant's delay has also meant that the first time many Class Members were confronted with confirmation that their data was taken during the Data Breach was when they were threatened by hackers via extortionate email, rather than finding out via adequate notice from Defendant and having the opportunity to implement mitigatory steps prior to being contacted by hackers.

131. Plaintiffs and the Class seek all available relief under RCW 19.255, including damages and injunctive relief.

FIFTH CAUSE OF ACTION
VIOLATION OF WASHINGTON'S UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
(On Behalf of Plaintiffs and the Class)

132. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above, as though fully stated herein.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

133. As a consumer of Defendant's services, Plaintiff is authorized to bring a private action under Washington's Unfair Business Practices--Consumer Protection law ("WUBPCP").

134. Plaintiff is a persons within the meaning of WUBPCP, which includes natural persons, corporations, trusts, unincorporated associations, and partnerships. RCW 19.86.010(1)

135. Plaintiff and the Class Members provided their PHI and PII to Defendant pursuant to transactions in "trade" and "commerce" as defined by WUBPCP, including the sale of services and any commerce directly or indirectly affecting the people of the state of Washington. RCW 19.86.010(2).

136. The WUBPCP prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." RCW 19.86.020

137. Plaintiff asserts this claim for Defendant's unfair and deceptive conduct, including its unlawful and unfair and deceptive acts and practices, which created a likelihood of confusion or of misunderstanding for Plaintiffs and members of the proposed Class.

138. Defendant engaged in unlawful, unfair, and deceptive acts and practices when it acquired and kept patients under the premise that any information those patients provided would remain protected and private, including but not limited to the following:

a. Failing to enact reasonable privacy and security measures to protect Plaintiff's and the Class PHI and PII from unauthorized disclosure, release, data breaches, malware, and theft;

b. Negligently representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and the Class's PHI and PII from unauthorized disclosure, release, data breaches, malware and theft, given the inadequacy of its privacy and security protections; and

c. Negligently failing to disclose the material fact of its unreasonably inadequate privacy and security protections.

139. The above unfair and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

the consumers could not reasonably avoid. Plaintiff's substantial injury outweighs any conceivable benefits to consumers or to competition.

140. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and the Class's PHI and PII considering the strong risk of a data breach. Through engaging in the above-named deceptive acts and practices, Defendant was negligent, knowing, and reckless with respect to the rights of members of the members of the proposed Class.

141. Plaintiff and the Class relied on Defendant to safeguard and protect their PHI and PII and to timely and accurately notify them if their data had been breached or compromised.

142. Plaintiff and the Class seek all available relief under the WUBPCP, RCW 19.86.090, including damages, the costs of the lawsuit, and reasonable attorneys' fees.

SIXTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
On Behalf of Plaintiffs and the Class)

143. Plaintiffs reallege and incorporates by reference every allegation contained in the paragraphs above, as though fully stated herein.

144. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

145. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

146. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed and continues to owe a legal duty to secure the sensitive information with which it is entrusted, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

147. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its clients' (*i.e.*, Plaintiff's and the Class's) data.

148. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

149. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

150. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment in his favor as follows:

151. Certification of the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and an order that adequate notice be provided to all Class Members;

152. Designation of Plaintiff as representative of the Class and the undersigned counsel, Zimmerman Reed LLP, as Class Counsel;

153. An award of damages in an amount to be determined at trial or by this Court;

154. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

155. An award of statutory interest and penalties;

156. An award of costs and attorneys' fees; and

157. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

The Plaintiffs hereby demand a trial by jury of all issues so triable.

Respectfully submitted,

Dated: December 14, 2023

/s/ Caleb Marker

Caleb Marker, WSBA #57112
ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
Telephone: (877) 500-8780
Facsimile: (877) 500-8781
caleb.marker@zimmreed.com

Brian C. Gudmundson (*Pro hac vice* forthcoming)
Charles R. Toomajian (*Pro hac vice* forthcoming)
Michael J. Laird (*Pro hac vice* forthcoming)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
charles.toomajian@zimmreed.com
michael.laird@zimmreed.com

Christopher D. Jennings
(*Pro hac vice* forthcoming)
JOHNSON FIRM
610 President Clinton Avenue, Suite 300
Little Rock, Arkansas 72201
Telephone: (501) 372-1300
Facsimile: (888) 505-0909
chris@yourattorney.com

Attorneys for Plaintiffs and the Proposed Class